La promesa y las trampas de DeFi





**Las finanzas descentralizadas podrían apoyar una nueva infraestructura financiera si se superan los desafíos**

La innovación digital ha traído importantes mejoras al sistema financiero. Pero la arquitectura del sistema sigue siendo esencialmente la misma. Todavía está centralizado.

Las finanzas descentralizadas (DeFi) ofrecen una alternativa. Utiliza redes públicas de blockchain para realizar transacciones sin tener que depender de proveedores de servicios centralizados como custodios, cámaras de compensación centrales o agentes de custodia. En cambio, estos roles son asumidos por los llamados contratos inteligentes.

Los contratos inteligentes son instrucciones en forma de código informático. El código se almacena en cadenas de bloques públicas y se ejecuta como parte de las reglas de consenso del sistema. Los protocolos DeFi se pueden diseñar de una manera que prohíba la intervención y la manipulación. Todos los participantes pueden observar las reglas antes de participar y verificar que todo se ejecute en consecuencia. Los cambios de estado (por ejemplo, actualizaciones de los saldos de las cuentas) se reflejan en la cadena de bloques y pueden ser verificados por cualquier persona.

En el contexto de DeFi, los contratos inteligentes se utilizan principalmente para garantizar la transferencia atómica (simultánea e inseparable) de dos activos o para mantener una garantía en una cuenta de depósito en garantía. En ambos casos, los activos están sujetos a las reglas del contrato inteligente y solo se pueden liberar si se cumplen las condiciones predefinidas.

Haciendo uso de estas propiedades, DeFi puede mitigar el riesgo de contraparte y replicar numerosos servicios financieros sin la necesidad de intermediarios y operadores de plataformas centralizadas. Esto puede reducir los costos y el potencial de errores. Los mercados de préstamos, los protocolos de cambio, los derivados financieros y los protocolos de gestión de activos son solo algunos ejemplos.

Los contratos inteligentes pueden hacer referencia a otros contratos inteligentes y hacer uso de los servicios que proporcionan. Si, por ejemplo, un protocolo de gestión de activos utiliza un intercambio descentralizado, los activos entrantes se pueden intercambiar como parte de la misma transacción. Este concepto, de acciones a través de múltiples contratos inteligentes que pueden tener lugar dentro de una sola transacción, se conoce como "componibilidad intra-transacción" y puede mitigar efectivamente el riesgo de contraparte (la probabilidad de que otras partes no cumplan con su parte del trato).

**Beneficios de la descentralización**

Muchas ventajas generalmente atribuidas a DeFi, o blockchains en general, también se pueden lograr a través de una infraestructura centralizada. Los contratos inteligentes no se limitan a los sistemas descentralizados. De hecho, los mismos estándares y entornos de ejecución se pueden utilizar en libros de contabilidad centralizados. Hay innumerables ejemplos de la máquina virtual Ethereum (una máquina virtual que se ejecuta en todas las computadoras de la red blockchain y ejecuta contratos inteligentes) que se emplea junto con protocolos de consenso fuertemente centralizados. Del mismo modo, los mismos estándares de token y protocolos financieros se pueden utilizar en plataformas centralizadas. Incluso la componibilidad puede funcionar en tales sistemas.

Además, los sistemas centralizados bien administrados son mucho más eficientes que las cadenas de bloques públicas. Eso podría llevar a la conclusión de que las cadenas de bloques públicas y DeFi son inferiores a los sistemas centralizados.

Sin embargo, los sistemas centralizados se basan en una suposición muy fuerte: la confianza en intermediarios e instituciones que son en gran medida opacas. Pero esa confianza no debe darse por sentada. La historia proporciona innumerables ejemplos de corrupción y errores dentro de las instituciones. Sin embargo, cuando los economistas discuten la infraestructura financiera y comparan las propiedades de las cadenas de bloques públicas con las de los libros de contabilidad centralizados, generalmente asumen que las entidades centralizadas son benévolas, lo que dificulta ver los beneficios de la descentralización.

Las cadenas de bloques públicas son transparentes. Debido a que no están controlados por una sola entidad, pueden proporcionar una infraestructura neutral, independiente e inmutable para las transacciones financieras. El código se almacena y ejecuta en un sistema abierto. Todos los datos están disponibles y son verificables. Esto permite a los investigadores y formuladores de políticas analizar transacciones, realizar estudios empíricos y calcular métricas de riesgo en tiempo real.

Lo más importante es que el acceso no está restringido. Esto tiene dos implicaciones.

En primer lugar, la ausencia de restricciones de acceso proporciona una base neutral que no puede discriminar entre casos de uso ni partes interesadas. Esto está en marcado contraste con los libros de contabilidad autorizados, cuyas reglas son establecidas por una entidad centralizada. Debido a que está tan centralizado, los estándares universalmente aceptados pueden ser difíciles de lograr, y los derechos de acceso y uso de la infraestructura podrían politizarse fácilmente. En previsión de tales problemas, los participantes que sientan que esto puede ser una desventaja para ellos no utilizarán la infraestructura centralizada en primer lugar. Los sistemas descentralizados pueden mitigar estos retrasos, lo que podría prevenir el problema de la falta de cooperación o de una cooperación mínima.

En segundo lugar, DeFi se basa en una infraestructura en capas (véase Schär 2021). Un libro mayor descentralizado no significa que todo lo que se implemente encima de él deba ser igualmente descentralizado. Puede haber buenas razones para que el acceso a ciertos tokens o protocolos financieros esté restringido o sujeto a intervención. Estas restricciones se pueden implementar a nivel de contrato inteligente sin comprometer la neutralidad general de la infraestructura base. Sin embargo, si el libro mayor en sí (capa de liquidación) ya estuviera centralizado, sería imposible descentralizar de manera creíble cualquier cosa construida sobre él.

Es muy probable que veamos un movimiento hacia libros de contabilidad que combinen pagos, activos tokenizados y protocolos financieros, como intercambios y mercados de préstamos. DeFi es el primer ejemplo de este desarrollo, pero habrá desarrollos similares en la infraestructura centralizada. La razón es que la componibilidad intra-transacción funciona sólo si los activos y los protocolos financieros están en el mismo libro mayor. Hay fuertes efectos de red, y ni los criptoactivos ni las monedas digitales del banco central serían particularmente convincentes si se implementaran en un libro mayor sin otros activos o protocolos financieros. Es posible crear una infraestructura centralizada componible con activos adicionales y protocolos financieros, pero sería arriesgado y difícil de gobernar dados los desafíos asociados con los libros de contabilidad autorizados. Esto es un argumento sólido a favor de la descentralización.

**Los sistemas centralizados se basan en una suposición muy fuerte:**

**la confianza en los intermediarios**

**Desafíos y riesgos**

Hay muchas ventajas que se pueden obtener de DeFi, pero hay desafíos y compensaciones que deben considerarse.

Primero, existe el riesgo de engaño, o "teatro de descentralización". Lo que generalmente se conoce como DeFi es, de hecho, a menudo fuertemente centralizado. En muchos casos, los protocolos DeFi están sujetos a fuentes de datos centralizadas y pueden ser moldeados o influenciados por personas con "claves de administración" o una asignación de tokens de gobierno altamente concentrada (derechos de voto). Si bien la centralización parcial no es necesariamente algo malo, es importante diferenciar estrictamente entre la verdadera descentralización y las empresas que afirman ser DeFi cuando en realidad proporcionan infraestructura centralizada.

En segundo lugar, la inmutabilidad puede introducir nuevos riesgos. Puede ser más difícil hacer cumplir la protección de los inversores, y los errores de programación de contratos inteligentes pueden tener consecuencias devastadoras. La componibilidad y los complejos esquemas de envoltura de tokens (Nadler y Schär, de próxima aparición) que se asemejan a la rehipotecación de garantías contribuyen a la propagación de choques en el sistema y pueden afectar a la economía real.

En tercer lugar, la naturaleza transparente de la cadena de bloques y la creación descentralizada de bloques pueden ser problemáticas desde una perspectiva de privacidad. Además, permite la extracción de rentas a través de la ejecución frontal generalizada, un fenómeno conocido como valor minero / máximo extraíble (MEV). Aquellos que observan una transacción que contiene una orden para intercambiar activos en un intercambio descentralizado pueden intentar ejecutar (o intercalar) esta acción emitiendo una transacción propia. De este modo, el favorito se beneficia a expensas del emisor de la transacción original. Existen soluciones potenciales que pueden mitigar al menos parcialmente este problema, pero implican compensaciones.

Finalmente, el escalado de las cadenas de bloques públicas no se puede hacer fácilmente sin comprometer algunas de sus propiedades únicas. La creación descentralizada de bloques inflige costos severos. Los requisitos de hardware para ejecutar un nodo no pueden ser arbitrariamente altos, ya que esto pondría precio a muchas partes interesadas y comprometería la descentralización. Esto limita la escalabilidad en cadena, lo que aumenta las tarifas de transacción. Esta compensación entre seguridad, descentralización y escalabilidad generalmente se presenta como un trilema. Una solución potencial es la llamada Capa 2s. Estos están diseñados para alejar parte de la carga de la cadena de bloques al tiempo que permiten a los participantes hacer valer sus derechos en la cadena de bloques en caso de que algo salga mal. Este es un enfoque prometedor, pero, en muchos casos, todavía requiere confianza y varias formas de infraestructura centralizada.

DeFi todavía se enfrenta a muchos desafíos. Sin embargo, también puede crear una infraestructura independiente, mitigar algunos riesgos de las finanzas tradicionales y proporcionar una alternativa a la centralización excesiva. La naturaleza de código abierto de DeFi fomenta la innovación, y hay muchas personas talentosas, académicos y profesionales por igual, que trabajan en estos desafíos. Si pueden encontrar soluciones sin socavar las propiedades únicas en el núcleo de DeFi, podría convertirse en un bloque de construcción importante para el futuro de las finanzas.



**FABIAN SCHÄR**es profesor de tecnología de contabilidad distribuida y fintech en la Universidad de Basilea y director general del Center for Innovative Finance.

Las opiniones expresadas en artículos y otros materiales son las de los autores; no reflejan necesariamente la política del FMI.

**Referencias:**

Schär, Fabián. 2021. "[Finanzas descentralizadas: en los mercados financieros basados en blockchain y contratos inteligentes](https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets)". Banco de la Reserva Federal de St. Louis Review 103 (2): 153–74. https://doi.org/10.20955/r.103.153-74.

Nadler, Matthias y Fabian Schär. Próximo. "¿[Finanzas descentralizadas, propiedad centralizada? Un proceso de mapeo iterativo para medir la distribución de tokens de protocolo](https://arxiv.org/abs/2012.09306)". Revista de Investigación Blockchain. https://arxiv.org/abs/2012.09306.